Claims

The following is claimed:

1-26. (canceled)

27. (currently amended) A computer-implemented method for creating a signature for subsequent authentication comprising:

indicating to a user commencement of signature input recording;

~~creating a signature by at least in part~~ recording user input signals by type from at least one user-selected device among a plurality of selectable user input devices,

wherein a signal comprises a set of related software-recognizable data of the same type received from at least one input device, and

wherein at least one user-selectable input device affords recording a plurality of signal types, and

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device;

terminating said recording;

creating a signature based at least in part upon said recording; and

storing said signature.

28. (previously presented) The method according to claim 27, wherein said recording comprises signals from a plurality of user-selected devices.

29. (previously presented) The method according to claim 27, further comprising receiving user selection of at least one signal type from a plurality of signal types associated with at least one user input device.

30. (previously presented) The method according to claim 27, further comprising passively terminating authentication comparison of a subsequent signature submission to said recording,

thereby authenticating said subsequent signature; and

wherein said signature comprises at least in part signal input that is user-controllable in duration.

31. (previously presented) The method according to claim 27, further comprising:

comparing a subsequent signature submission to said recording,

and accepting said comparison within a predetermined degree of inexactness,

thereby authenticating said subsequent signature.

32. (previously presented) The method according to claim 31, wherein said predetermined degree comprises a user-designated tolerance.

33. (previously presented) The method according to claim 27, further comprising presenting at least a portion of said recording to said user for editing,

wherein said recording does not entirely comprise text-character codes.

34. (previously presented) The method according to claim 27, further comprising editing said recording,

wherein said signature is not entirely comprised of text-character codes.

35. (currently amended) A computer-implemented method for creating a signature for subsequent authentication comprising:

receiving user selection of at least one signal type among a plurality of selectable signal types;

recording input data of at least one signal type from at least one user-selected input device among a plurality of selectable user input devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user-selectable input device,

and wherein at least one user-selectable input device affords recording a plurality of signal types; and

creating a signature comprising at least in part at least a portion of said input data of said user-selected signal types; and

storing said signature.

36. (previously presented) The method according to claim 35, wherein said recording comprises a plurality of user-selected devices.

37. (previously presented) The method according to claim 35, such that said recording precedes said receiving signal type selection.

38. (previously presented) The method according to claim 35, wherein at least one said signal type comprises input from a plurality of devices.

39. (previously presented) The method according to claim 35, further comprising:

comparing a subsequent signature submission to said recording,

and accepting said comparison within a designated tolerance of inexactness,

thereby authenticating said subsequent signature.

40. (previously presented) The method according to claim 35, further comprising editing said recording,

wherein said signature is not entirely comprised of text-character codes.

41. (previously presented) The method according to claim 35, wherein said recording comprises a plurality of user-selected signal types.

42. (currently amended) A computer-implemented method for incrementally authenticating a signature while receiving user input comprising:

receiving a first portion of user input data;

accumulating keys based upon matching correspondingly key data to said first portion of user input data,

wherein a key comprises at least in part a portion of a previously stored signature,

wherein said signature divisible into portions,

wherein said keys associating portions sequentially either integrally or by reference;

subsequently, iteratively receiving a plurality of portions of user input data and performing a corresponding authentication step for each portion,

~~wherein the first authentication step upon receiving a first portion of said user input comprises accumulating keys based upon matching correspondingly key data to said first portion of user input data,~~

~~wherein a key comprises at least in part a portion of a previously stored signature, said signature divisible into portions, said keys associating portions sequentially either integrally or by reference,~~

wherein, upon receiving each subsequent portion after said first portion, discarding from further processing previously accumulated keys based upon failure in matching respective key data to said user input data portion; and

whereby continuing said iterative process until completing authentication by matching said last key to corresponding said user input data portion, or by process of elimination determining authentication impossible.

43. (previously presented) The method according to claim 42, wherein accepting said match within a designated tolerance of inexactness.

44. (previously presented) The method according to claim 42, wherein accessing at least one key by reference from another key.

45. (previously presented) The method according to claim 42, wherein said first portion comprises input from a plurality of devices.

46. (previously presented) A computer-implemented method for storing the signatures of a plurality of users comprising:

recording a plurality of signatures comprising data of a plurality of transmission types and signal types,

wherein a transmission type comprises indicia of a user-selected input device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device, and

wherein at least two signals types are associated with at least one single input device; and

partitioning said signature data by transmission type and by signal type.

47. (previously presented) The method according to claim 46, further comprising storing a signature at least in part by partitioning said signature into portions by signal type,

such that at least one portion references another portion of said signature.

48. (previously presented) A computer-implemented method for creating a signature comprising:

recording user input of a plurality of signal types from at least one user-selected device among a plurality of user-selectable devices,

wherein a signal type comprises a category, among a plurality of possible categories, of measurable variable input associated with at least one user input device;

receiving user selection among those signal types recorded,

whereby receiving user selection of at least one less signal type than recorded for said device;

creating a signature comprising at least in part said user-selected signal types.

49. (previously presented) The method according to claim 48, further comprising receiving user indication to edit said signature,

wherein said signature is not entirely comprised of text-character codes.